SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

An Overview of SAFECode & its Current Work on In-house Security Engineering Training

Stacy Simpson (stacy@safecode.org)
Dan Reddy, CISSP (reddy_dan@EMC.com)

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Agenda

- SAFECode Update
- Overview of Best Practices for

  In-house Security Engineering Training

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Software Assurance Today

- Individual companies are implementing better methods for developing and delivering more secure software, hardware and services…

but…

- Industry lacked a common framework or trusted forum to advance or share these effort

Software Assurance:
Confidence that software, hardware and services are free from intentional and unintentional vulnerabilities and that the software functions as intended.

Introducing SAFECode

- The Software Assurance Forum for Excellence in Code (SAFECode) was announced on 23rd October 2007

- SAFECode is the first global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

SAFECode Brings Together SMEs

- SAFECode unites subject matter experts with unparalleled experience in managing complex global processes for software development, integrity controls and supply chain security.
- The goal is not to establish one way but to identify methods that work and can be effectively leveraged in a rational way by governments and enterprises.

SAP
symantec
Microsoft
Juniper NETWORKS
EMC² where information lives®
NOKIA

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

SAFECode Objectives

- Increase understanding of the secure development methods and integrity controls used by vendors
- Promote proven software assurance practices among vendors and customers to foster a more trusted ecosystem
- Identify opportunities to leverage vendor software assurance practices to better manage enterprise risks
- Foster essential university curriculum changes needed to support the cyber ecosystem
- Catalyze action on key research and development initiatives in the area of software assurance

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Fundamental Practices for Secure Software Development

- A list of fundamental practices in use by SAFECode members
- A highly practical and actionable document; model for future work
- It's short!
  - Only 22 pages
- Not an academic research document
- Software development process agnostic

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

An Industry Consensus Document

Microsoft

symantec.

NOKIA

EMC²
where information lives®

SAP

Juniper NETWORKS

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Document Contents

- Implemented SAFECode member practices that fit into the “rhythm of the business”
- Each section includes explanation and references for secure development during:
  - Design
  - Programming
  - Testing
  - Code Integrity and Handling
  - Documentation

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Whitepaper has been popular; feedback extremely positive

- Software assurance is dynamic; planning yearly update of document
- Will open document to public comment via web site during Q2
- Updated document will published in Q4

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Other 2009 Priorities

- Software Supply Chain Assurance
- Software Assurance R&D
- Product Measurability

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Current Project

- In-house Security Engineering Training
  - Still collecting feedback; paper currently being reviewed by International Advisory Board
  - Like other work, based on a detailed analysis of member programs and approaches
  - Difficult to develop standard practices given training's direct relationship with unique corporate environment
  - Framework approach used to outline common findings

IT and Communications Vendors

who develop internal SwA* programs find that:

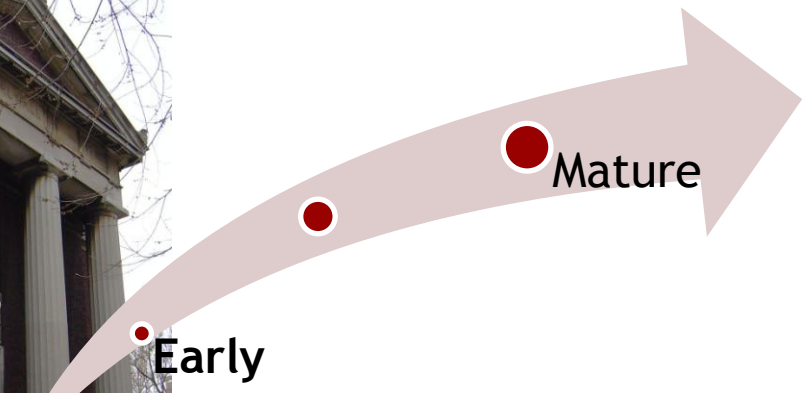
Fundamental to their success

- The people who are designing, developing, testing and delivering software must understand the fundamentals of secure software engineering that lead to secure practices and products

** Software assurance encompasses methods and processes that ensure software functions as intended while mitigating the risks of vulnerabilities and malicious code that could bring harm to the end user.*

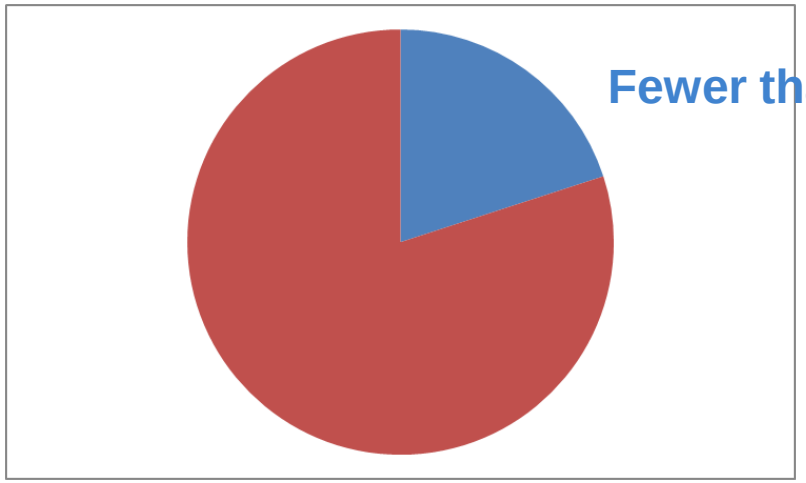
Today's reality:

- Member companies have leveraged internally developed training programs
  - Only way to build specialized skills and knowledge to support their own organization's s unique development environment
- University programs for building secure software are still in



Secure development principles are not yet a significant part of the software engineering curriculum at the university level.

- UK 2008 data says that computing graduates lack security skills



Fewer than 20% properly trained

Cyber Security
Knowledge Transfer Network

A qualitative 2008 survey by the Cyber Security Knowledge Transfer Network concluded that fewer than 20 percent of UK computing undergraduates get a meaningful education in secure development and design.

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

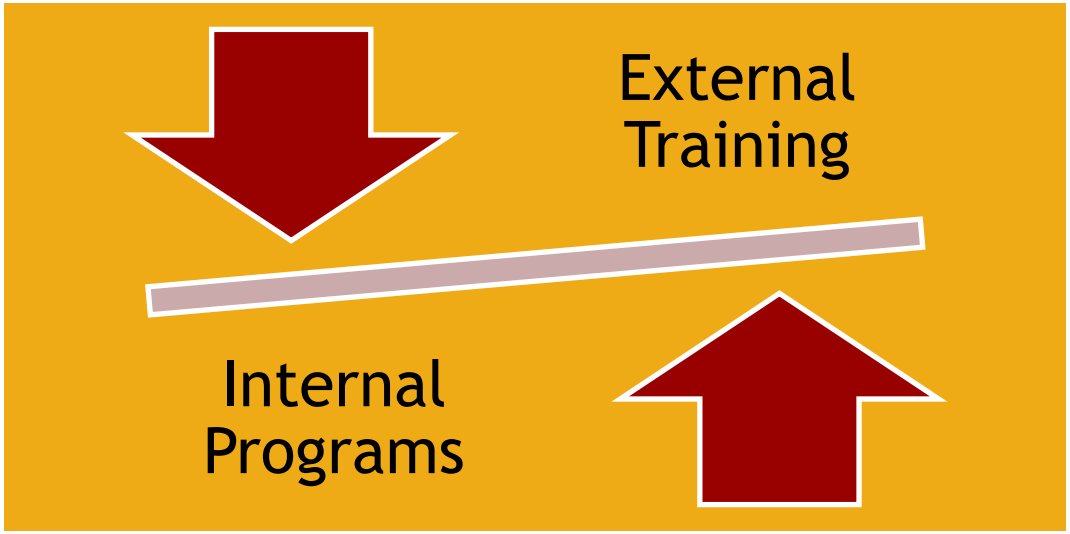
Not outlining a curriculum rather…

suggesting a framework

- Specialized
- Advanced
- Foundational

A Framework for:
Internal Security
Engineering Training

This debate is not taken lightly…



- Fact
  - Shortage of sufficient SW Engineers who possess security skills
- Could consider outsourcing part of training
  - …but content may not relate to the organization's unique development environments, processes and security policies
  - Some tailoring is usually needed anyway

- SAFECode advocates University training
  - In both full-time programs

& Continuing Education

- External training and professional certification programs add value
  - Many programs fill an important need for specialized technical training for certain segments of development teams
  - Professional certification bring knowledge into companies and are incentives for an individual's career.
  - (SAFECode is not endorsing any particular programs)
    - Examples listed as resources

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Define Training Goals

- Content should create an understanding of basic security such as:
  - Secure Design Principles
  - Secure Coding Principles
  - The Most Common Errors that Lead to Security Vulnerabilities
  - Threat Modeling
  - How to Find / Test Security-related Issues in Code
  - How to Fix Security Issues etc.
  - Security in the company's Software Development Lifecycle

1011010
0010100

A conceptual understanding of security issues should include buffer overflows, data validation, SQL injection, cross site scripting, format string vulnerabilities and use of unsafe functions or behaviors, etc.

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Define Training Targets

- Target a Broad Internal Audience
  - Spread awareness of software security
    - Develop “Security-aware” culture & mindset
  - Develop advocates in Engineering
  - Target all who touch products !!!

SAFECode member companies believe that the basics of security engineering need to be understood by everyone involved with software development including Product Managers, Product Architects/ Designers, Program/ Project Managers, Development Engineers and Quality Assurance (QA) Engineers.

- **Foundational**
  - Topics like:
    - Basic understanding of the current threat environment and the important role of secure development practices in attack prevention
    - Include topics like business risks/rationale, internal standards and policies, basics of secure coding and testing
    - Overview of a company's approach to security in the development lifecycle

- **Advanced**
  - Topics like:
    - Language & OS specific techniques to prevent and fix software vulnerabilities
    - Secure design principles
    - Secure testing methodologies
    - Secure coding techniques
    - Find and fix security flaws against common definitions (e.g. CWE,CVE)
    - Threat modeling techniques

Audience:

Dev Managers,
QA
Developers

- **Specialized**
  - Role-based
  - Directly tied to job functions
    - Security tools
      - e.g. specific static code analysis tool
    - Common Criteria workshops

- Developing Training Content is an Ongoing Effort
  - While some of the skills / knowledge required are static; others need constant education.
  - It is important to develop an understanding of the ever-changing, dynamic threat

  - Many SAFECode members supplement their internal training programs with informal approaches:
    - podcasts, newsletters, in-house conferences, webinars, guest speakers, etc. to keep product teams updated on security developments.

Training Program Implementation

- Must be relevant to work at hand
- Sensitive to corporate culture
- Mandated vs. Professional Development
- Must reward people; develop incentives
- Keep direct link between content and performance

- Time is most the precious commodity
  - Customized and adaptable
  - Applying the techniques lead to less time to fix errors
  - Tailor to product development cycles

- Computer Based Training vs. Instructor Led Training debate
  - Depends on: company's unique attributes, size, culture, distribution
  - SAFECode members: Adopt Hybrid

Computer Based	Instructor Led
Flexible Schedule	Get direct answers
Cost Effective	May accommodate labs
Suited for global orgs	In-house mentoring
Can intermix COTS content	Build peer resources

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Training Framework

- Measurement
  - Tie training measurement to corporate goals
    - and Individual Performance
  - Direct and in-direct measurements
    - How many team members have been training?
    - How is training being received by learners?
    - Has it affected quality of output – i.e. teams with more trained engineers produce code with fewer vulnerabilities than those teams with less

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Conclusion

- In-house training essential to success
  - Industry must drive its own improvements; can't afford to wait for someone else to train workforce
- But not a replacement for university-level training
  - Industry must continue to work with universities to address gaps in security engineering training

Questions ???

SAFECode Contact:

Stacy Simpson, Policy Director
stacy@safecode.org
+ 1 703-812-9199
www.safecode.org

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

SAFECode members:

EMC²
where information lives™

Juniper NETWORKS

Microsoft

NOKIA

symantec.

SAP

SAFECode.org is a comprehensive online resource for news and information about software assurance.

SAFECode members include EMC Corporation, Juniper Networks, Inc., Microsoft Corp., Nokia, SAP AG, and Symantec Corp.